Listing of Claims

Claims 1-39 (canceled)

Claim 40 (previously added): A method for determining secret information contained in a first cryptography device using a second cryptography device, the method comprising the steps of:

a. generating an electrical signal comprising a stream of bits containing a correct digital signature in said first cryptography device;

b. transmitting the electrical signal containing the correct digital signature to said second cryptography device;

c. placing said first cryptography device under physical stress and in response to the physical stress, generating an electrical signal comprising a stream of bits containing an incorrect digital signature in said first cryptography device;

d. transmitting the electrical signal containing the incorrect digital signature to said second cryptography device;

e. in a processor in said second cryptographic device, determining secret information q stored in said first cryptography device using:

$$\gcd(E-\hat{E},N) = q$$

wherein N is a product of prime numbers, and one of the prime numbers is q; and

f. generating an output electrical signal comprising a stream of bits containing the secret information used to generate the correct signature.

Claim 41 (previously added): The method of claim 40 wherein said first cryptographic device generates a digital signature which may be separated into linear components.

Claim 42 (previously added): The method of claim 40 wherein placing said first cryptography device under physical stress includes at least one of applying atypical voltage levels, applying a higher speed than said first cryptography device was designed to accommodate, or applying radiation.

Claim 43 (previously added): A method for determining secret information contained in a first cryptography device using a second cryptography device, the method comprising the steps of:

a. in said first cryptography device, generating an electrical signal comprising a stream of bits containing a first authentication value of form r^2 mod N wherein r is a random number and N is a secret value which is a product of prime numbers and transmitting said electrical signal containing the authentication value to said second cryptography device;

b. in said second cryptography device, generating an electrical signal comprising a stream of bits containing a subset of integers S and transmitting said electrical signal containing the subset of integers to said first cryptography device;

c. in response to receipt of the electrical signal containing the subset of integers, generating in said first cryptography device an electrical signal comprising a stream of bits containing a second authentication value of form $\hat{y} = (r + \acute{E}) \Pi_{i \in s} s_i$ wherein $\hat{y}$ is an erroneous value, s_i is a secret exponent used to encrypt, and $\acute{E}$ is a value added to r due to an error and transmitting said second authentication value to said second cryptography device;

d. in response to receipt of the electrical signal containing the second authentication value, determining in a processor of said second cryptography device a value for $\acute{E}$ by computing:

$$\left(r + \acute{E}\right)^2 = \frac{\hat{y}^2}{\Pi_{i \in s} v_i} (\mathrm{mod}\, N)$$

wherein $v_i = s_i^2$;

f. determining in the processor of said second cryptography device a value of r by computing:

$$\left(r + \acute{E}\right)^2 - r^2 = 2\acute{E}r + \acute{E}^2 (\mathrm{mod}\, N);$$

g. in response to the calculated values of $\acute{E}$ and r, determining in the processor of said second cryptography device a value for s_i by computing:

$$\Pi_{i \in s} s_i = \frac{\hat{y}}{r + \acute{E}} (\mathrm{mod}\, N); \text{ and}$$

h. generating an output electrical signal comprising a stream of bits containing secret information $\Pi_{i\in S} s_i$.

Claim 44 (previously added): The method of claim 43 wherein the step of determining s_i further includes the step of computing in the processor in said second cryptography device:

$$\prod_{i\in S} s_i = \frac{2\acute{E}\,\hat{y}}{\frac{\hat{y}^2}{\prod_{i\in S} v_i} - r^2 + \acute{E}^2} (\mathrm{mod}\, N).$$

Claim 45 (previously added): The method of claim 43 further comprising the step of determining in the processor in said second cryptography device whether the value of É satisfies the relation $(y') = (r')^2 T^2$ by using the subset of integers S; wherein T is a guessed value for $\Pi_{i\in S} s_i$.

Claim 46 (previously added): The method of claim 43 wherein the step of generating the electrical signal comprising a subset of integers S in said second cryptography device includes generating a plurality of subsets of S.

Claim 47 (previously added): The method of claim 46 wherein the step of generating in said first cryptography device an electrical signal comprising a second authentication value in response to receipt of the signal containing the plurality of subset of S further includes generating a second authentication value for each subset S of the plurality of subsets S received.

Claim 48 (previously added): The method of claim 47 wherein the step of generating a plurality of subsets S in said second cryptography device further comprises generating singleton sets.

Claim 49 (previously added): A method for determining secret information contained in a first cryptography device using a second cryptography device, the method comprising the steps of:

a. placing said first cryptography device under physical stress and in response to the physical stress, generating an electrical signal comprising a stream of bits containing an incorrect digital signature in said first cryptography device;

b. transmitting the electrical signal containing the incorrect digital signature to said second cryptography device;

c. in response to receipt of the electrical signal containing the incorrect digital signature, selecting a block length in a processor of said second cryptography device;

d. determining in the processor of said second cryptography device a candidate vector w that matches all known bits of the secret information and is zero elsewhere by computing:

$$w = \sum_{y=k_i}^{n} s_j 2^j + \sum_{j=k_i-r}^{k_i-1} u_j 2^j$$

wherein k_i is a time at which an error may have occurred; s_j is a bit which may be incorrect; r is a possible blocklength; and u is a bit which may be incorrect;

e. determining in the processor of said second cryptography device whether candidate vector w is correct by computing:

$$\exists e \in \{0,\ldots,n\} s.t. \left(\hat{E}_j \pm 2^e m_j^W\right)^{e_j} = m_j \pmod N$$

wherein e = a public exponent;

n = a number of bits in the secret information;

m_j = a message;

e_j = a public signature verification exponent; and

N = a product of prime numbers;

f. if the candidate vector w is correct, generating an output electrical signal comprising a stream of bits containing a value for the selected block length; and

g. if the candidate vector w is incorrect, determining in the processor of said second cryptography device another candidate vector.

Claim 50 (previously added): The method of claim 49 wherein the steps (c) – (f) are performed for a plurality of block lengths.

Claim 51 (previously added): A method for determining secret information contained in a first cryptography device using a second cryptography device, the method comprising the steps of:

a. generating in said second cryptography device an electrical signal comprising a stream of bits containing a challenge t and transmitting the electrical signal containing the challenge to said first cryptography device;

b. in response to receipt of the electrical signal containing the challenge t, generating in said first cryptography device an electrical signal comprising a stream of bits containing a response of form $u = r + ts \bmod p$, wherein:

r is a random number selected by the first cryptography device;

s is the first cryptography device's secret key; and

p is a large prime number;

c. transmitting the electrical signal containing a response to said second cryptography device;

d. transmitting the electrical signal containing the same challenge t to said first cryptography device;

e. in response to receipt of the electrical signal containing the challenge t, generating in said first cryptography device an electrical signal comprising a stream of bits containing a second response of form $\hat{u} = \hat{r} + x \bmod p$, wherein:

$\hat{r}$ is an erroneous value of r and x is $ts \bmod p$;

f. in response to receipt of electrical signal containing the second response, determining in said second cryptography device a location of the error; and

g. generating an output electrical signal comprising a stream of bits containing the secret integer s_i.

Claim 52 (previously added): The method of claim 51 wherein the step of determining the location of the error further comprises the steps of trying all possible locations of the error.